IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

KAJEET, INC.,	§	
	§	
Plaintiff,	§	Case No. 6:21-cv-389-ADA
	§	
v.	§	**JURY TRIAL DEMANDED**
	§	
TREND MICRO INC.,	§	
	§	
Defendant.	§	

DEFENDANT TREND MICRO INC.'S REPLY MEMORANDUM IN SUPPORT OF MOTION TO DISMISS UNDER FEDERAL RULE 12(B)(6) FOR FAILURE TO STATE A CLAIM

TABLE OF CONTENTS

TABLE OF AUTHORITIES

I. INTRODUCTION

The question of infringement in this case is cut and dried. Trend Micro Inc. ("Trend Micro") knows how its Accused Products work. In its opening brief, Trend Micro showed in detail how the very Product Guide[1] attached to Kajeet, Inc.'s ("Kajeet") Complaint showed that the Accused Products involved only locally stored policies. Kajeet does not contest that the statements in the Product Guide accurately describe how the Accused Products operate. Notably, neither the Product Guide nor anything else cited in Kajeet's Complaint even mentions the existence of a "remote server," much less a system in which "a policy [is set or] stored at the server" and user device communication is "enabled or disabled without storing the policy on the computing device" by enforcing a "decision" that is "receiv[ed] in real-time from the server" as the claims of U.S. Patent No. 8,667,559 ("the '559 Patent") require.[2] (*See, e.g.*, Dkt. No. 1 at ¶¶ 18, 34-37, Dkt. No. 1-1 at 18:38-53). Had Kajeet done its proper pre-filing diligence by, for example, testing the publicly available Accused Products, it would already know those limitations are not met.

Because the speculative allegations in Kajeet's Complaint that contradict the evidence in the Product Guide must be discounted, its infringement claim should be dismissed as not "plausible on its face." *See Bot M8 LLC v. Sony Corp.. of Amer.*, ___ F.3d ___, 2021 WL 2932690, at *7-*8 (Fed. Cir. July 13, 2021) (dismissing infringement claim where allegations about product contradicted claim requirement that authentication program be stored separate from motherboard). Kajeet warps this standard when it asks: "Where in the Product Guide is there a statement that the policies are stored on the device rather than on a Trend Micro server?" (Dkt. No. 14 at 10). The

[1] Excerpts from the "Trend Micro Security 2021 for Windows Product Guide" ("Product Guide") are attached to the Complaint as Exhibit C. (Dkt. No. 1-3).

[2] Although identifying claims 1 and 27 in its original Complaint, Kajeet served Preliminary Infringement Contentions on July 19, 2021 that identified only claim 27 as asserted. Accordingly, the discussion herein focuses on claim 27, although for all relevant purposes as claim 1 has a similar scope, the arguments likewise apply to claim 1.

standard for dismissal is not so high as to require an explicit statement in the language of the patent. Pleading facts that are "inconsistent with and contradict infringement" warrant dismissal. *Id.* at *8. Kajeet's supposition that the statements in the Product Guide merely relate to policy *selection* is also not plausible. To implement control over a managed device using the Accused Products, the Product Guide directs the user to download and "install Trend Micro Security/Mobile Security ***on that device***" and then walks an administrator through the steps for setting and configuring policies on that device—a point that Kajeet does not dispute. (*See generally* Dkt. No. 8 at 7-10, Dkt. No. 14 at 9-10). Kajeet even acknowledges that the portions of the Product Guide that instruct an administrator to set the policies on the managed device "confirm" how the policies are set by administrators and "the steps taken to do so." (Dkt. No. 14 at 10). If the configuration instructions were actually being set and stored on a remote server, as Kajeet posits, there would be no reason to require the administrator to perform the configuration from the managed device—any network-connected device would do. Moreover, Kajeet offers no explanation for how policies could be set from the managed device without also storing them on the device at least for some short time.

Perhaps in recognition of these deficiencies in its Complaint allegations, Kajeet attempts to rely on a new document (which it refers to as "the Product Guide for the iOS version of the Accused Products") that was not attached to its Complaint. (*Id.* at 11). As an initial matter, reliance on that document is improper. But even when this other document is considered, it shows nothing to dispel the inconsistency between Kajeet's allegations about how the Accused Products meet the claim limitations and how those products actually work.

Nor do Kajeet's arguments regarding Section 101 fare better. Kajeet's contention that it should be allowed to pursue its infringement claim even if it encompasses systems in which policies are stored on the managed device flies in the face of the claim language. Contrary to

Kajeet's argument that "the limitations present in the asserted claims do not go so far as to require that all policies may only be stored at the server" (Dkt. No. 14 at 15 (emphasis removed)), claim 27 explicitly requires that the policy cannot be stored on the managed device: "the communication being enabled or disabled ***without storing the policy on the computing device***." (Dkt. No. 1-1 at 18:51-53). For this very reason, Kajeet has admitted before other courts that "the parties cannot reasonably dispute the plain claim language that shows that ***the claimed policy and claimed enforcement step*** in Claim 27 of the '559 Patent ***occur remote from the computing device***." (Dkt. No. 8-1 at 13). Kajeet cannot now reverse course to plead infringement on the one hand, while still avoiding a finding of invalidity under Section 101 on the other.

II. Kajeet's Infringement Claim Should Be Dismissed with Prejudice in Light of the Factual Evidence Contained in Its Pleadings

Where, as here, it would be futile for Kajeet to amend its Complaint, dismissal with prejudice is appropriate. (Dkt. No. 14 at 18 (citing *Foman v. Davis*, 371 U.S. 178, 182 (1962) for the proposition that "futility of amendment" is a valid reason to deny leave to amend)). The manner in which the Accused Products operate is clear and immutable, as are Kajeet's admissions as to what is required for infringement, and no amendment to its allegations can change the facts that the Accused Products simply do not use a remote server to set or store policies or send access decisions back to the managed device or that policies are stored on the devices themselves.

A. Kajeet's Allegations that the Accused Products Set, Store and Apply Policies at a Remote Server Are not Plausible in Light of the Product Guide

Under the *Iqbal*/*Twombly* pleading standard, "[w]here … factual allegations are actually *inconsistent* with and contradict infringement, they are likewise insufficient to state a plausible claim." *Bot M8*, 2021 WL 2932690, at *8 (emphasis in original). Claim 27 of the '559 Patent requires that the policy used to decide whether a managed computing device's communication request is granted or denied must be "stored at a server" "without storing the policy on the computing device." (Dkt. No. 1 at ¶¶ 18, 34-37, Dkt. No. 1-1 at 18:38-53). Kajeet likewise alleges that "[t]he policies for defining permissible or impermissible uses of the devices *are set and stored at the Trend Micro server* by parents or administrators using the Trend Micro Mobile Security app." (Dkt. No. 14 at 6-7 (citing Dkt. No. 1 at ¶ 24)) (emphasis added).

The Product Guide attached to Kajeet's Complaint shows that the Accused Products do not meet these limitations. It describes a process of configuring parental control policies that requires the user to first download and install an application on the managed device and then have a parent or administrator set and configure policies from the device itself. (*See, e.g.,* Dkt. No. 8-4 at 16, 38, 165-179 and discussion of same at Dkt. No. 8 at 6-10, 13-15). Kajeet does not challenge this explanation of what the Product Guide shows. (Dkt. No. 14 at 10 (acknowledging that the cited portions of the Product Guide "confirm that policies for 'restrict[ing] a child's access to certain activities or content' are set by administrators (i.e., parents) and show the steps taken to do so.")). Indeed, Kajeet's acknowledgement that the Product Guide describes at least local (on-device) setting of policies is a departure from the allegations in its own Complaint and is in direct contradiction to its infringement allegations. (*See* Dkt. No. 1 ¶¶ 18 ("In accordance with certain embodiments of the inventions disclosed, ***the policies are set and stored at the server level*** to provide simultaneous control over use of one or more mobile communication devices.")). The only plausible conclusion to draw from the Product Guide's explanation of the configuration of the Accused Products is that policies are ***stored on the managed device itself***, contrary to the claim limitation "without storing the policy on the computing device." (Dkt. No. 1-1 at 18:52-53) (emphasis added).

Faced with similar facts in *Bot M8*, the Federal Circuit affirmed a district court's dismissal of plaintiff's claims of patent infringement with prejudice where the patent claims required that authentication software be stored "*separate* from the 'motherboard' and its memory" and the complaint included a factual allegation that the accused products stored authentication software on the motherboard. *Bot M8*, 2021 WL 2932690, at *8 ("That allegation renders [plaintiff's] infringement claim not even possible, much less plausible.").

Instead of addressing why the Product Guide's instruction to set the policies for a user on the managed device (i.e., not on a server) is consistent with its infringement allegations, Kajeet speculates that the Accused Products could still utilize remote storage of policies even though parents/administrators are required to use the managed device itself to configure policies for controlling that device. Aside from being inconsistent with the way these Accused Products actually work, Kajeet's assumptions about such an operating scenario are implausible in light of the facts presented, and not presented, in the Product Guide. The Product Guide makes no mention of a remote server on which policies are stored. If a parent or administrator was simply using the managed device to set a policy that is stored on a remote server, then the Product Guide should also be expected to provide instructions on how the parent or administrator could set or access such server-stored policies from other networked devices connected to the server (e.g., when the device is being used by the user/child). But the Product Guide tellingly makes no mention of those things, because despite Kajeet's conjecture, that is simply not how the Accused Products operate.

B. Kajeet's Reference to the iOS Product Guide Is Inappropriate and Irrelevant

Kajeet's reference to another product guide (for an Apple iOS product) that was not included in its Complaint should not change the Court's conclusion.[3] It is entirely proper for the

[3] Kajeet's characterization of the document as "available at the same URL listed in paragraph 27 of the Complaint" is misleading. The URL (https://helpcenter.trendmicro.com/en-us/?_ga=2.9052341.1823008893.1611956421-1531980936.1611178202) is to a general Help Center page on Trend Micro's website and does not include a specific link for the document Kajeet cites. *Greg Young Publg., Inc. v. CafePress, Inc.*, CV 15-06013-MWF-AJWX, 2016 WL 6106752, at *2 (C.D. Cal. Jan. 25, 2016) (refusing to incorporate by reference information found outside of "FAQs" section on website that was quoted in complaint as it was "not a blanket permission to incorporate unrelated information found elsewhere on Defendant's domain.").

Court to consider documents attached to a pleading as evidence in deciding a motion to dismiss because the exhibits are considered part of the complaint "for all purposes." *See U.S. ex rel. Riley v. St. Luke's Episcopal Hosp.*, 355 F.3d 370, 376 (5th Cir. 2004) (quoting Fed. R. Civ. P. 10(c)); *Lone Star Fund V (US), LP v. Barclays Bank PLC*, 594 F.3d 383, 387 (5th Cir. 2010). However, documents presented by Kajeet outside its pleading and for the first time in its opposition to Trend Micro's motion to dismiss, like the iOS product guide on which Kajeet now relies, should not be considered. *Dorsey v. Portfolio Equities, Inc.*, 540 F.3d 333, 338 (5th Cir. 2008) (in deciding a motion to dismiss, the Court "may rely on only the complaint and its proper attachments").

But even if the Court considers this document, it does nothing to change the fact that the portions of the iOS product guide Kajeet cites do not address the storage of policies at any remote server. And like the Product Guide Kajeet attached to its Complaint, the iOS product guide explains that the operation of the software requires that an application be downloaded and installed onto the managed device and that a parent/administrator set policies for the managed device on the device itself. (Dkt. No. 14-2 at 10-11, 21-27). Kajeet points to excerpts from the document that indicate a VPN is established when parental controls are in use. (Dkt. No. 14 at 11-13). But while the establishment of a VPN suggests that data may be transferred to and from the device, it does not support an inference that *policies* are specifically transmitted from the device to a remote server or that a remote server applies policies and sends access *decisions* back to the device. The excerpts Kajeet cites say nothing about transmitting policies or the parent's/administrator's selections or receiving access decisions to block or enable the device's access requests.

III. Kajeet's Section 101 Argument Is Inconsistent with Its Infringement Argument

Kajeet does not contest the District of Delaware's finding in the *Gryphon* case that under step one of the *Alice* analysis, the asserted claims of the '559 Patent are directed to the abstract idea of "controlling access to and the functionality of a device." *Kajeet, Inc. v. Gryphon Online*

Safety, Inc., C.A. No. 19-2370 (MN), 2021 WL 780737, at *6-*7 (D. Del. Mar. 1, 2021). Nor does Kajeet contest that the sole reason the Delaware court found, at the pleading stage, that Kajeet's allegations were sufficient to avoid invalidation under Section 101 was that Kajeet had plausibly pled that "the claimed invention improves upon the prior conventional systems by ***remotely storing policies for controlling access to the computing device***." *Id*. at *7 (emphasis added).

But Kajeet's opposition confirms that now, contrary to its prior positions on Section 101 as well as the plain language of claim 27, Kajeet is arguing that the claims do not "require that ***all*** policies may ***only*** be stored at the server." (Dkt. No. 14 at 15). In other words, Kajeet is now arguing that even systems in which policies that apply locally (on-device) stored policies to managed device access requests fall within the scope of the claims (at least so long as some copy of the policy is also stored remotely). Kajeet's flip-flop in interpretation in order to argue infringement against Trend Micro runs squarely afoul of the prior *Qustodio* decision, which found that claims that did not require a "distributed architecture" in which the applied policies are stored remotely did not embody any inventive concept and failed *Alice* step two. *Kajeet, Inc. v. Qustodio, LLC*, Case No. 8:18-cv-01519-JAK-PLA (C.D. Cal. Nov. 1, 2019) Dkt. No. 140 (Dkt. No. 8-1 at 19 ("As noted, the claim construction determined that remote policy storage is not a required limitation of Claim 1 of the '371 Patent or Claim 1 of the '612 Patent. Therefore, Plaintiff's stated basis for patent eligibility at *Alice* Step Two in which it refers to the particular arrangement of claim elements to create a 'distributed architecture,' is again without force.")).

Kajeet's Complaint allegations and its arguments on Section 101 all hinge on its characterization of the claims as requiring this "distributed architecture," where policies are not stored on the managed device. It does not argue that a system in which policies are stored on, and applied by, managed devices themselves (even if copies of those policies are also stored remotely) embody the "distributed architecture" previously found to make the claims patent-eligible at the pleading stage.

In light of the prior *Qustodio* decision (Dkt. No. 8-1), Kajeet should be collaterally estopped from making such an argument now. *See, e.g.*, *Joao Control & Monitoring Sys., LLC v. Digital Playground, Inc.*, 12-cv-6781, 2016 WL 5793745, at *4-5 (S.D.N.Y. Sept. 30, 2016); *Cardionet, LLC v. The ScottCare Corp.*, 325 F.Supp.3d 607 (E.D. Pa. 2018). Collateral estoppel applies "when: (1) the identical issue was previously adjudicated; (2) the issue was actually litigated; and (3) the previous determination was necessary to the decision." *Pace v. Bogalusa City Sch. Bd.*, 403 F.3d 272, 290 (5th Cir. 2005) (*en banc*). "Preclusion applies when the party to be precluded had a full and fair opportunity to litigate the merits of the issue." *Blonder-Tongue Laboratories, Inc. v. Univ. of Ill. Found.*, 402 U.S. 313, 328 (1971); *Xitronix Corp. v. KLA-Tencor Corp.*, 916 F.3d 429, 439 (5th Cir. 2019). In *Qustodio*, Kajeet had a full and fair opportunity to litigate the patent eligibility of the claims of two patents related to the '559 Patent—U.S. Patent Nos. 8,712,371 and 8,630,612. The district court determined that the claims of those related patents "do not require a 'remote' relationship of policies compared to the claimed computing device and that "[t]hose determinations undermine statement that Plaintiff made … in the context of the parties' dispute under 35 U.S.C. 101." (Dkt. No. 8-1 at 18). The *Qustodio* court dismissed Kajeet's infringement claims as to those two patents after specifically finding that "[r]emote policy storage is critical and central … to support Plaintiff's patent eligibility arguments at *Alice* Step One." (*Id.* at 19 (citing Kajeet's arguments that "[t]he asserted claims require remote storage of usage policies which are thereby less vulnerable to manipulation by the user of the device(s) being managed while still accommodating real-time, continuous control during device usage," '[t]he claims are addressed to specific solutions in which the policies applied are stored remotely and are, therefore, inaccessible by the controlled device . . . These limitations capture the distributed architecture scheme resulting in improved effectiveness of the claimed systems," and "systems which require no communication to a remote component storing usage policies cannot be within the scope of the challenged claims.")). Yet here, Kajeet should be collaterally estopped from relitigating that very issue by arguing that the '559 Patent claims it now contends allow for on-device storage and application of policies are nevertheless patent-eligible.

IV. CONCLUSION

Trend Micro respectfully requests that Kajeet's Complaint be dismissed with prejudice for the foregoing reasons.

Respectfully Submitted,

/s/ Katherine P. Chiarello
Katherine P. Chiarello
Texas State Bar No. 24006994
katherine@wittliffcutter.com
WITTLIFF | CUTTER, PLLC
1209 Nueces Street
Austin, Texas 78701
(512) 649.2434 office
(512) 960.4869 facsimile

Charanjit Brahma (pro hac vice)
Benesch Friedlander Coplan & Aronoff LLP
One Market Street, Spear Tower
36th Floor
San Francisco, CA 94105
(628) 600.2241 office
(628) 221.5828 facsimile

Manish Mehta (pro hac vice)
Benesch Friedlander Coplan & Aronoff LLP
71 South Wacker Drive, Suite 1600
Chicago, IL 60606
(312) 212.4953 office
(628) 221.5828 facsimile

Attorneys for Defendant Trend Micro Incorporated

CERTIFICATE OF SERVICE

Pursuant to the Federal Rules of Civil Procedure and Local Rule CV-5, I hereby certify that, on July 26, 2021, all counsel of record who have appeared in this case are being served with a copy of the foregoing via the Court's CM/ECF system.

/s/ Katherine P. Chiarello
Katherine P. Chiarello